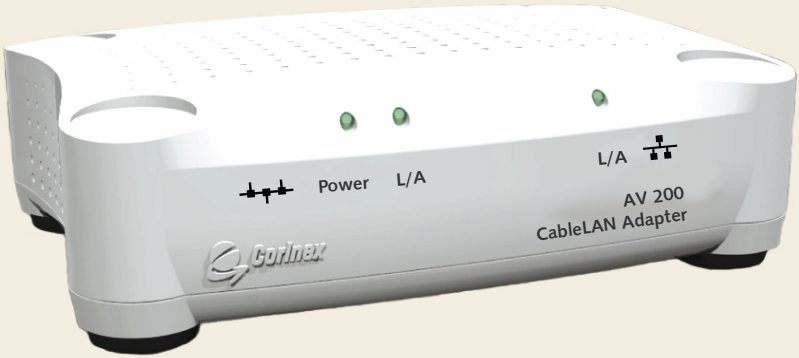
Corinex
AV200
CableLAN Adapter



Corinex

Manual

Published by:
Corinex Communications Corp.
#670-789 West Pender Street
Vancouver, B.C.
Canada V6C 1H2
Tel.: +1 604 692 0520
Fax: +1 604 694 0061

NOTE: This equipment has been tested and found to comply with the limits for Class B information technology equipment. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference, the end user is advised to take adequate measures.

2005-02-08 ver. 1

CORINEX COMMUNICATIONS CORPORATION

This End User License Agreement ("EULA") is a legal agreement between you and CORINEX COMMUNICATIONS CORPORATION ("CORINEX") with regard to the copyrighted Software provided with this EULA.

Use of any software and related documentation ("Software") provided with a CORINEX hardware product, or made available to you by CORINEX via download or otherwise, in whatever form or media, will constitute your acceptance of these terms, unless separate terms are provided by the software supplier, in which case certain additional or different terms may apply. If you do not agree with the terms of this EULA, do not download, install, copy or use the Software.

1. Licence Grant. CORINEX grants to you a personal, non-transferable and non-exclusive right to use the copy of the Software provided with this EULA. You agree you will not copy the Software except as necessary to use it on a single hardware product system. You agree that you may not copy the written materials accompanying the Software. Modifying, translating, renting, copying, transferring or assigning all or part of the Software, or any rights granted hereunder, to any other persons, and removing any proprietary notices, labels or marks from the Software is strictly prohibited. Furthermore, you hereby agree not to create derivative works based on the Software. You may permanently transfer all of your rights under this EULA, provided you retain no copies, you transfer all of the Software, and the recipient agrees to the terms of this EULA. If the Software is an upgrade, any transfer must include all prior versions of the Software.

2. Copyright. The Software is licensed, not sold. You acknowledge that no title to the intellectual property in the Software is transferred to you. You further acknowledge that title and full ownership rights to the Software will remain the exclusive property of Corinex Communications Corporation and/or its suppliers, and you will not acquire any rights to the Software, except as expressly set forth above. All copies of the Software will contain the same proprietary notices as contained in or on the Software.

3. Reverse Engineering. You agree that you will not attempt, and if you are a corporation, you will use your best efforts to prevent your employees and contractors from attempting to reverse compile, modify, translate or disassemble the Software in whole or in part. Any failure to comply with the above or any other terms and conditions contained herein will result in the automatic termination of this license and the reversion of the rights granted hereunder to CORINEX.

4. Disclaimer of Warranty. The Software is provided "AS IS" without warranty of any kind. CORINEX and its suppliers disclaim and make no express or implied warranties and specifically disclaim warranties of merchantability, fitness for a particular purpose and non-infringement of third-party rights. The entire risk as to the quality and performance of the Software is with you. Neither CORINEX nor its suppliers warrant that the functions contained in the Software will meet your requirements or that the operation of the Software will be uninterrupted or error-free.

5. Limitation of Liability. Corinex's entire liability and your exclusive remedy under this EULA shall not exceed the price paid for the Software, if any. In no event shall CORINEX or its suppliers be liable to you for any consequential, special, incidental or indirect damages of any kind arising out of the use or inability to use the software, even if CORINEX or its supplier has been advised of the possibility of such damages, or any claim by a third party.

6. Applicable Laws. This EULA will be governed by the laws of Canada, excluding its conflict of law provisions.

7. Export Laws. This EULA involves products and/or technical data that may be controlled under any applicable export control laws, and regulation, and may be subject to any approval required under such laws and regulations.

8. Precedence. Except as set out above, where separate terms are provided by the software supplier, then, subject to this EULA, those terms also apply and prevail, to the extent of any inconsistency with this EULA.

Contents

1 Introduction

1.1 Overview

The *Corinex AV200 CableLAN Adapter* is a network interface adapter which uses the coaxial cable lines already in your home or office as a medium for communication. After successful installation, the AV CableLAN network behaves like a traditional LAN for computers. The *Corinex AV200 CableLAN Adapter* supports network speeds of up to 200 Mbps .

The advantage of our product is that it keeps network maintenance costs low and eliminates usage barriers, while requiring no additional wiring. It is highly integrated, and requires no external electronic components.

The *Corinex AV200 CableLAN Adapter*:

- Enables users to connect individual PCs or other devices with Ethernet communications links into a local area network through existing coaxial cables
- Enables PC file and application sharing
- Enables peripheral and printer sharing through the CableLAN network
- Enables shared broadband Internet access
- Enables sharing of bandwidth for multimedia payloads, including voice, data, audio and video
- Eliminates the need for long network cables throughout your home or office
- A real, cost-effective, and reliable solution for high-speed communications in any home or small office

1.2 About this Manual

This User Guide includes everything you need to know to help you successfully install the *Corinex AV200 CableLAN Adapter* and meet your networking needs. With the information in this manual, you should be able to:

- Analyze your network efficiency
- Plan the configuration of your Corinex AV200 CableLAN Adapter
- Install and configure your Corinex AV200 CableLAN Adapter according to your plan
- Verify and optimize the performance of your Corinex AV200 CableLAN Adapter

2 Installation Guide

2.1 What this Package Contains

When you receive your *Corinex AV200 CableLAN Adapter*, check to be sure that your package contains:

- Corinex AV200 CableLAN Adapter
- Power cable
- Coaxial cable
- Coaxial splitter
- Straight-forward Ethernet cable
- Printed Manual (this document)
- CD with documentation

We are constantly innovating our products. For the latest hardware/software changes, downloads, and additional information on your device, please visit **www.corinex.com**.

We also advise you to visit our Corinex Authorized Partners Program web page **http://cappp.corinex.com/**, where you can find valuable information about complex applications and installations, as well as partners in your area who can provide installation services.

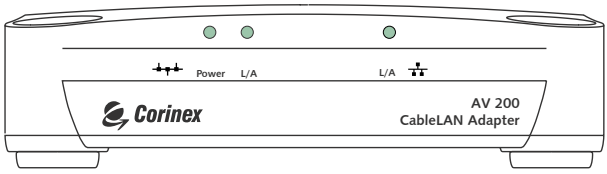
2.2 System Requirements

- IBM compatible PC or a Macintosh
- One available 10/100 Mbps Ethernet port
- Windows 98/ME/2000/NT/XP, Mac OS X or Linux operating system
- Javascript compatible web browser for configuration (Netscape, Internet Explorer, Opera…)

2.3 Front Panel Description

LED Definitions

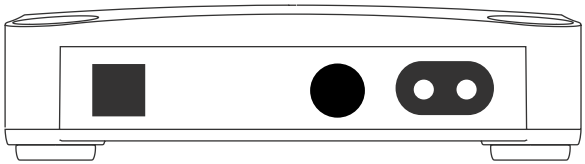
(LEDs from left to right)



1. POWER	Green	On: Power on Off: Power off
2. Link/Activity	Green	Off : No cable activity Blinking : Receiving/Transmitting data
3. ETHERNET	Green	Off: No link on LAN On: Link on LAN Blinking: receiving/transmitting data

2.4 Rear Panel Description

Connector Definitions
(Connectors from left to right)



1. LAN: 1x RJ-45 LAN10/100 Fast Ethernet port
2. CableLAN: 1xF-Type connector
3. Power cord: Power supply

Standards Compliance	IEEE 802.3u, UPA pre-standard
Speed	Up to 200 Mbps on physical layer
AC Plug Type	US, EU, UK and AUS
LED Status Lights	Power, Link/Activity (coaxial cable), Ethernet Link
Interface	10/100BaseT Fast Ethernet, F-Type
Frequency Range used	2 – 34 MHz
Power Input	85 to 265 V AC, 50/60 Hz
Dimensions	148 mm L x 106 mm W x 47 mm H
Transmitted Power spectral density	-56 dBm/Hz
Power Consumption	5W
Safety & EMI	UL/FCC Part 15, CB/CE and/or international standards approved

2.6 Installing the AV200 CableLAN Adapter

To connect the *Corinex AV200 CableLAN Adapter* to your computer, follow the steps listed below.

1. Connect the supplied Ethernet cable to the LAN port on the adapter and to an Ethernet port on your computer.
2. Connect the power cable to the adapter and the other end into any AC electrical outlet.
3. Connect the coaxial cable to the adapter and to any coaxial plug

Note: Please use a straight-forward Ethernet cable for connection of the AV200 CableLAN Adapter to your computer. If you are connecting the AV200 CableLAN Adapter to a modem or switch, please use a crossover cable.

2.7 Testing the Setup

To verify that your equipment is connected and working correctly, use the standard **Ping** utility. In Windows, click on menu **Start -> Run**, then write the command **ping IPADDRESS -t**, where IPADDRESS is the IP address of the computer to which the AV200 CableLAN Adapter is connected, e.g. **ping 192.168.4.1 -t** (this process can be interrupted by pressing **CTRL+C**).

1. Ping the IP address of the computer to which the AV200 CableLAN Adapter is connected. If this fails, there is a problem with the Ethernet network card or with the TCP/IP protocol.
2. Repeat the same process with the other computers on your AV200 CableLAN network.
3. If all the computers can ping themselves, try pinging another computer on your AV200 CableLAN network. If this fails, then there is a problem with the connection across your AV200 CableLAN network or with the configuration of the AV200 CableLAN Adapters. Check the connection to the coax plug, or try a different jack. Verify the configuration of the AV200 CableLAN Adapters, especially the network number, as only adapters in the same network can see each other. Please see chapter 3 for details on configuration.

If you experience any problems with your setup, try unplugging the AV200 CableLAN Adapter and restarting the computer, as this sometimes fixes the problem. If the problem persists, please refer to the troubleshooting guide at the end of this manual.

3 Web Configuration

In order to access the web configuration pages, it is necessary to know the adapter's IP address and to be connected to it (e.g. through an Ethernet cable). Adapters that have not previously been configured have the IP address **10.10.1.69**. Open a web browser (Microsoft Internet Explorer v6.0, Mozilla v1.7.2 and Mozilla Firefox v1.0 have been verified for use with these products.), and type the IP address in the address bar – the URL should be **http://10.10.1.69/** unless you are not setting it up for the first time, and you have previously changed it to something else.

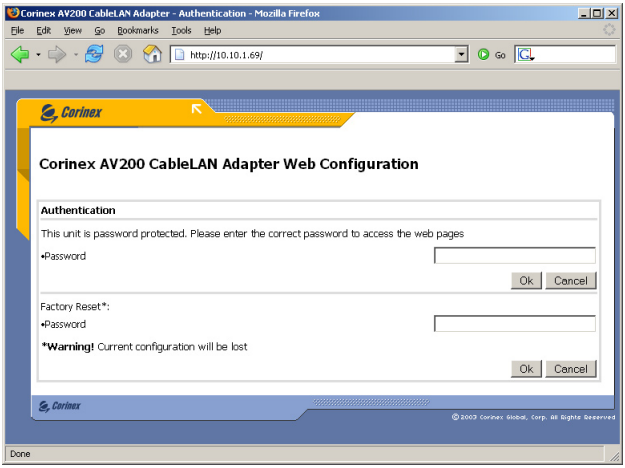
Changing the default IP address, **10.10.1.69**, is required to allow access to an adapter when two or more units are active on the same network. The IP address is a device's unique identifier on a network, so the adapters would not be able to tell each other apart if they had the same identity, just as a postman wouldn't know which house to deliver to, if two neighbors in a large city had the same street number. Follow the steps below to configure a new IP address for each adapter:

1. In your computer's network settings, enter an address in the range 10.10. X.X and the netmask 255.255.0.0. This is necessary in order to be compatible with the adapter's default settings. For details on how to set up an IP address in your computer, please see chapter 5.
2. Plug in your AV200 CableLAN Adapter and connect it to the PC via the supplied Ethernet cable.
3. Open the Web browser and type the following URL: **http://10.10.1.69**. You will get to the configuration web interface of the AV200 CableLAN Adapter.

3.1 Authentication Page

If the configuration password is enabled, you'll need to login before you can access the web pages where you make changes to the network. Therefore, you will first be taken to an **Authentication** page, where you will need to enter either the configuration password – to access these web pages or a factory reset password – in order to set the configuration to a default value. The embedded web server has an authentication timeout of 5 minutes; i.e. if no web pages are loaded within 5 minutes, the login expires and you will need to login again.

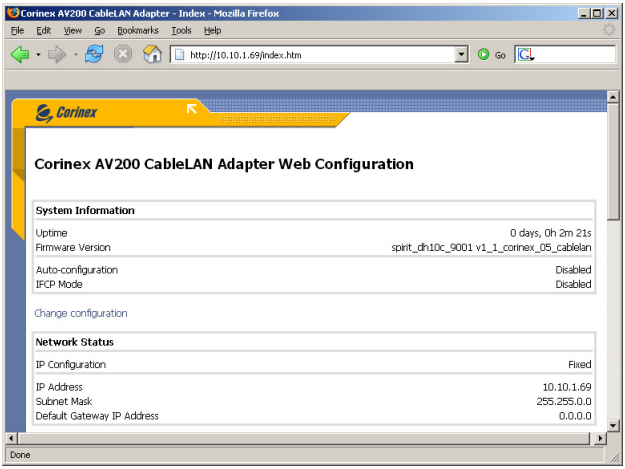
Note: The default password for accessing the configuration is "**paterna**". The default password for resetting the adapter into default settings is "**betera**".



Note: If password protection is disabled, you will be taken straight to the **Main** page instead of the Authentication page.

3.2 Main Page

This is the first page after login, or simply the first page if the configuration password is disabled. It shows the current settings and some basic information about your adapter. Selecting **Change Configuration** will load the **Change Configuration** page.



3.3 Change Configuration Page

3.3.1 Overview

This configuration page lets you set some of the adapter's basic options. Any settings changed here will be stored in the adapter's permanent memory and loaded and configured automatically as soon as the adapter is restarted. Changing these settings also takes effect immediately, with the exception of a few particular options.

Notes:

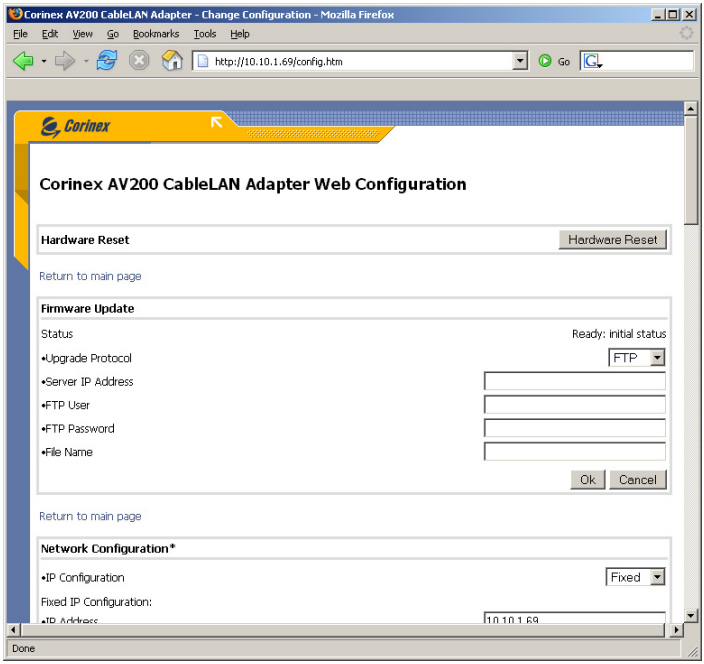
- A different IP must be set for each adapter that will operate on the same network. An adapter's IP does not need to be in the same range as the devices or PCs communicating with the adapters. Only while accessing the configuration page, a PC must have the same address range as the adapter (10.10.X.X and Netmask 255.255.0.0 in the default state).

- The adapter's netmask can also be changed, for example to a type C (255.255.255.0) if necessary. This is a more advanced option, which you may ignore if you're not familiar with it.

- If the adapter is going to be accessed through a router (for example in a large office network), the gateway IP needs to be configured. Otherwise, it can be ignored.

THE IP CHANGE IN THE ADAPTERS WILL BE EFFECTIVE ONLY AFTER A RESTART OR A REBOOT. IT MAY BE A GOOD IDEA TO PLACE A LABEL ON EACH ADAPTER WITH ITS IP ADDRESS, SO YOU DON'T LOSE THE ABILITY TO ACCESS IT.

WARNING: If you change the IP and forget it, there is no way to reset it to the default value. This may imply sending the unit back for reprogramming.



3.3.2 Hardware Reset

Clicking on this button will reset, or reboot, your adapter.

3.3.3 Firmware Update

Should you need to update the firmware, first select the protocol: **FTP** or **TFTP**. Then enter the IP address of the FTP or TFTP server (**Server IP Address** field). Then enter the file name of the firmware image (**File Name**) which you will have provided via download, or possibly CD. If you're using FTP, enter the user name (**FTP User**) and password (**FTP Password**). Finally, press **Ok**. The browser will load a different page, the **Firmware Update** page (see section 3.4), which will show the status of the firmware update.

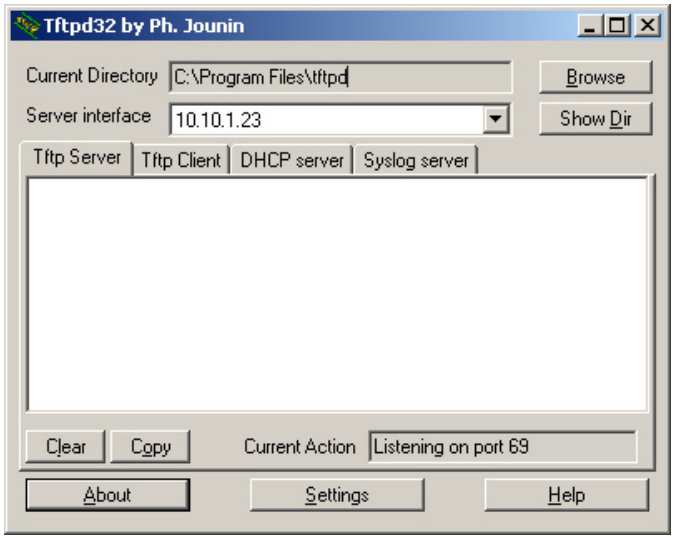
3.3.4 Firmware upgrade using a TFTP Server

To upgrade the firmware of the modem using TFTP, a TFTP server must be running on a computer. We recommend a freeware tool called **TFTPD32**. This tool can be downloaded at the following address: **http://tftpd32.jounin.net/**.

The firmware image is provided by Corinex. Check that the name of the image file matches the platform (dh10) and type of chip (9001, 9010) that is being upgraded.

Follow the steps below to upgrade the firmware of a modem:

1. Execute **TFTPD32**. This application has the GUI shown in the picture below.

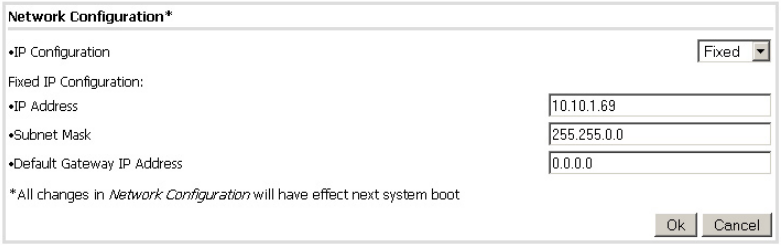


2. Place the image file in the directory specified in **Current Directory** or change it to point to the place where the image is stored.
3. Open the Web browser and enter the IP of the modem that to be upgraded.
4. When the page comes up, click on **Change configuration**.
5. In the **Firmware Update** window, select TFTP and enter the IP of the TFTP server and the name of the image file, as shown in the next picture.
6. Click **Ok** to start the process. Progress information is shown on the Web page every 30 seconds.
7. The modem will first download the file and then calculate the CRC.
8. If the CRC is correct, the **Hardware Reset** button will be highlighted. The modem must be reset for the new firmware to start running.

3.3.5 Network Configuration

The modem in your *Corinex AV200 CableLAN Adapter* can be configured to use DHCP or a fixed IP (IP Configuration).

The following settings are used by the fixed IP configuration. In order to use the adapter in conjunction with other equipment, on a P2P or an In-Home AV network, it is necessary to define a valid and unique IP address on the network, as well as a proper subnet mask and gateway address. These options will be stored in the modem and activated at each reboot or restart.

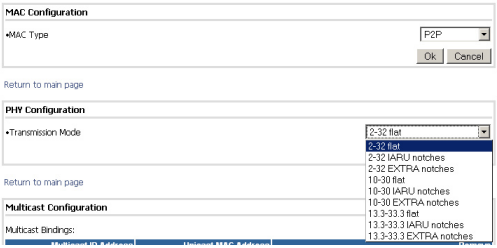


3.3.6 MAC and PHY Configuration

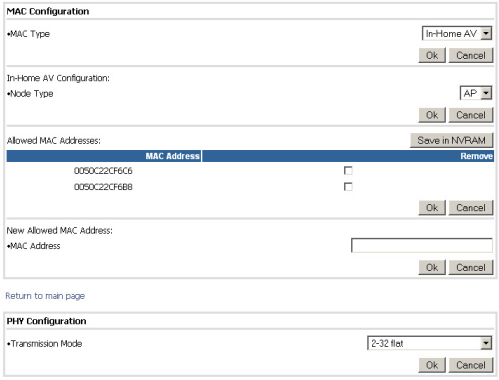
The following settings are in regards to the type of network you want to set up. The *Corinex AV200 CableLAN Adapter* supports two different types of networks: **P2P** and **In-Home AV** (**MAC Type** checkbox). Chapter 4 contains more information about the types of network setups.

> **Note:** The user is strongly recommended to use the In-home AV mode as this can significantly increase the performance and security. We cannot guarantee the presence of the P2P mode in the future versions of the AV200 firmware.

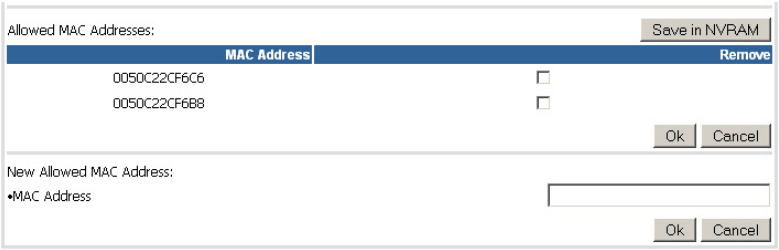
Regardless of which type of network you choose, the spectral notches must be either enabled or disabled (**Transmission Mode** selector). If the adapter is running in an environment where it can cause interference to a HAM radio receiver, the option of spectral masking can be enabled. When this option, called **2-32 MHz with Notches**, is enabled, it blocks the CableLAN signal entirely from the frequency bands used by HAM radio.



When using an In-Home AV network, further configuration is possible. An adapter can be defined as either an Access Point (**AP**) or an End Point (**EP**) (**Node Type** field).



The settings for an Access Point (**AP**) include a list of the allowed End Point MAC addresses, the other adapters that are allowed to connect to the Access Point. The list can be saved directly to the adapter (**Save in NVRAM**). You can remove MAC addresses by checking their **Remove** checkboxes and clicking **Ok**. A new MAC address can be added to the list by entering it, in hexadecimal format in the appropriate field and clicking **Ok**.

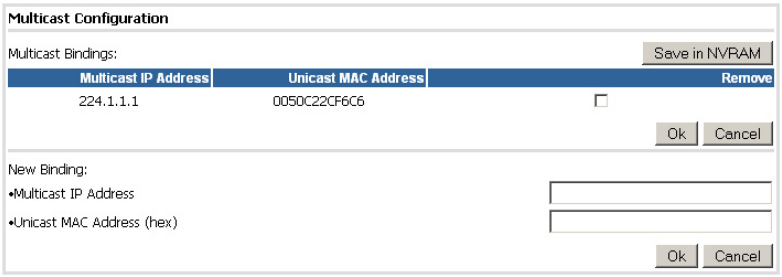


For the configuration to become effective, click **Ok** and wait for the page to refresh. The modem does not need to be rebooted.

3.3.7 Multicast Configuration

In order to optimize multicast traffic (video streams, etc.) between the AV200 powerline devices, the user can specify which devices will receive the traffic. All others will not be able to listen to the multicast communication therefore the bandwidth originally used for transmission will be preserved.

This form shows the list of multicast bindings, where multicast IP addresses are tied to a unicast MAC address. This list can be saved to the adapter (**Save in NVRAM**). Moreover, you can remove bindings by checking their **Remove** checkboxes and clicking **Ok**. A new binding can be added to the list by entering the multicast IP address, in decimal (*ddd.ddd.ddd.ddd*) format, and the unicast MAC address, in hexadecimal (*XXXXXXXXXXXX*) format, in the suitable fields and clicking **Ok**.

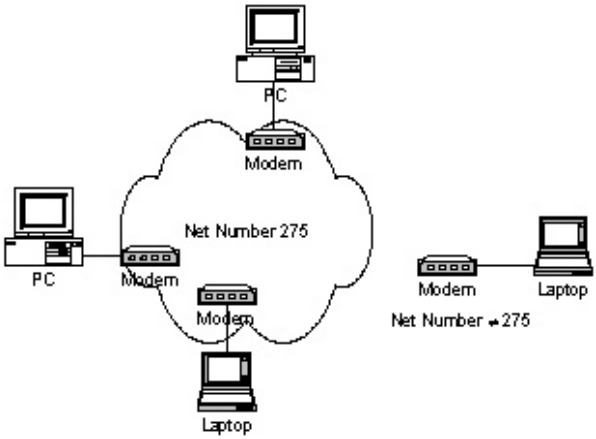


3.3.8 Security Configuration

The web application lets you change the configuration password by typing a new password (twice, for verification). If both fields are left empty, the configuration password will be disabled and the message **No password installed** will be shown in the security configuration form. This means the web configuration authentication (login to these web pages) will be disabled too. The authentication can be enabled again by simply entering a configuration password at any time.

The ***Network Identifier*** can also be set as a hexadecimal (*xxxxxx*) value. It should have the same value on each adapter within a single network. This number (between 1 and 220-1) will be used to encrypt your CableLAN transmissions. Entering **000000** (six zeroes) disables the encryption.

Adapters with different **Network Identifiers** are not able to communicate with each other. The purpose of this basic encryption scheme is not to offer tight security restrictions; but is designed as a simple way of differentiating between in-home networks, a way to keep your computers separated into different networks, or groups, according to your needs.

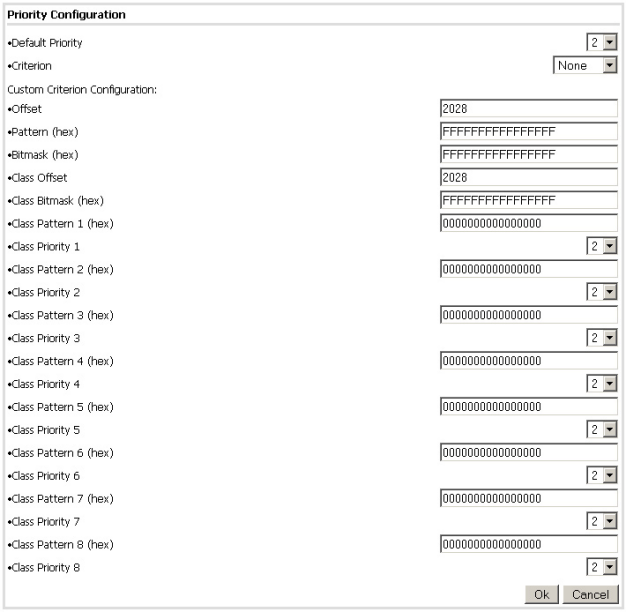


In order to initiate a factory reset, a specific password is required. If the password is valid, the configuration will be set back to factory defaults.

3.3.9 Priority Configuration

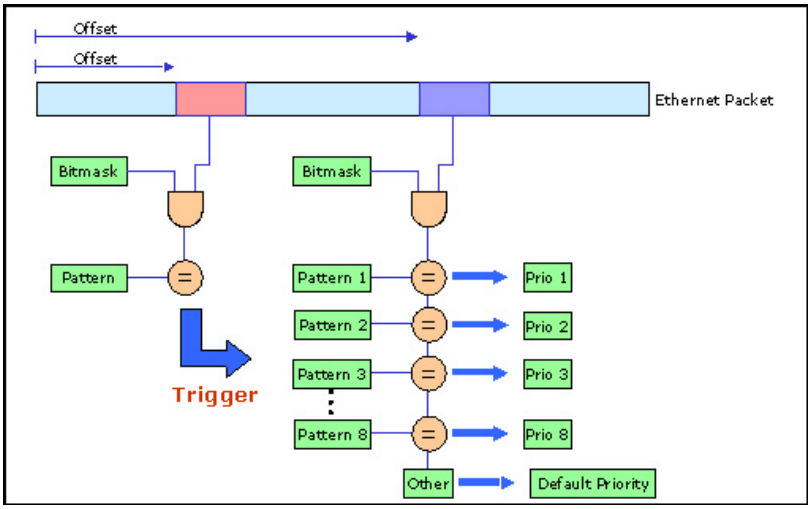
Several options are available in this form. These parameters let you configure the Quality of Service criterion. The first, and easiest to understand and use, is the **Default Priority** value. Data output from adapters with a higher default priority will have a higher preference in the network, and their data will be delivered before others.

If you select **None**, **8021p** or **TOS** from the drop-down menu, subsequent **Custom** options are ignored and the default settings are used. To enter customized options, select **Custom** from the menu and proceed with your settings.



When several traffic flows are sharing the same network, there is sometimes the need to establish several levels of priority to guarantee that bandwidth-sensitive applications such as video or telephony continue to work smoothly even under network congestion.

The traffic classifier is a packet inspector that is able to recognize several patterns inside an Ethernet frame and assign a different priority to each of them. To ensure that the classification is done to the right type of packet, there is a trigger mechanism preceding the actual classification. The trigger mechanism is also based on pattern recognition in a given location of the Ethernet packet. The next picture depicts the packet classification mechanism.



There is one offset, one bitmask and pattern for the trigger condition. The trigger condition is useful to make sure that the Ethernet frame contains, for example, an IP frame. To check this condition, the offset would need to be set to 16 and the bitmask to 0xFFFF. If the resulting pattern is 0x0800, then the Ethernet frame contains an IP packet and the classification can be done to a known field.

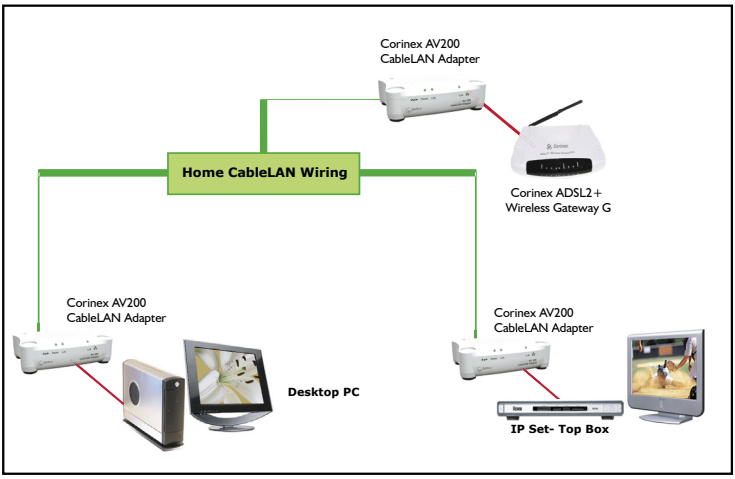
There is another offset and bitmask for the classification condition. The resulting value is compared with a set of patterns. If the value matches a given pattern, the packet will be classified with the specified priority. If the value does not match any of the patterns, it will get a default priority.

There is a set of pre-defined criteria that allow classifying traffic based on the **802.1p** field of the Ethernet packet or the **TOS** field of the IP packet.

3.3.10 Configuring Video Applications

In the case of a network where real-time traffic must coexist with massive data transfers, the service classifier must be used to prioritize the bandwidth-sensitive traffic above the other types of traffic.

As an example, consider the network shown below.



The node connected to the ADSL modem is the access point. Data and video are delivered through ADSL. The access point has to prioritize UDP video over data to avoid a jittery image when there is a heavy data download.

First of all, the **Criterion** field must be set to **Custom**, in order to create one's own rules to classify the traffic.

To prioritize UDP traffic, first the Ethernet packets containing IP packets have to be detected. This requires detecting the pattern 0x0800 at offset 16. Because the field to inspect is two bytes, the bitmask must also cover the same space. Therefore, 0xFFFF is used as bitmask. These values are introduced in the fields **Custom Criterion Offset**, **Custom Criterion Pattern** and **Custom Criterion Bitmask**.

Once the trigger condition is entered, the classification rules must be specified. Only the fields that are actually changed will take effect. The rest will be ignored. IP packets have a one-byte field at offset 27 that indicates the *Protocol Type*. UDP protocol is pattern 0x11. Because the field to inspect is only one byte, the bitmask is also one byte. The values are entered in the first available rule (1) as **Class Pattern 1** and **Class Priority 1**.

The rest of the traffic (FTP, Web browsing, etc.) will receive default priority 2. On the other side of the network, the modem connected to the computer will also classify outgoing data traffic with default priority 2 because no rule has been programmed.

> **Note:** While the offset value is assumed to be decimal, the patterns and the bitmasks are in hexadecimal format by default.

3.4 Firmware Update Page

This page appears when a firmware update is requested from the **Change Configuration** page, and it shows the status of the current firmware update. The **Firmware Update** page is reloaded automatically every 30 seconds. When the status line shows **Ready: finished correctly**, the adapter can be restarted, and the new firmware will be loaded.

If the update process fails, an error message will be shown. In this situation, the adapter can be reset without any risk, but the old firmware will still be present on the adapter.

4 Network Topologies – Peer-to-Peer, Server/Client

4.1 Peer-to-Peer

If **P2P** is selected in the **MAC** configuration form, the adapter will act as a **Peer-to-Peer** node, allowing direct connections between computers. In a **P2P** network, all the adapters communicate directly with each other, without a central server, and they share the available space on a single channel. Automatic repeating is performed to allow communication between nodes that do not have direct visibility. Configuration is simpler, because all of the nodes have the same settings (except the IP).

In order to setup a new **P2P** network, it is only necessary to configure every adapter in your network with the following:

- A unique private **IP** (e.g. 10.10.1.<last MAC address byte>)
- The MAC mode set to **P2P**
- **Notches** set to the same option as on all other adapters on your network (either enabled or disabled)
- All adapters in a P2P network must have the same **network identifier** set.

To add a new computer to your P2P network, simply set these three options on the adapter to the same settings, the only difference being in the last digits of the IP address.

> **Note:** The user is strongly recommended to use the In-home AV mode as this can significantly increase the performance and security. We cannot guarantee the presence of the P2P mode in the future versions of the AV200 firmware.

4.2 In-Home AV

An **In-Home AV** network is made up of an "access point" and several "end points," or one server and several clients, up to a maximum of 32 end points per access point. An **In-Home AV** network can have only one server (access point). However, you can have several networks running simultaneously in the same home or office, because each server (access point) is isolated from the others by a unique network identifier, and the clients (end points) can only communicate with the server to which they are configured via their MAC addresses.

The adapters are optimized for this mode and perform better in terms of both network speed and security, therefore the the In-home AV mode is preferred and recommended for all users.

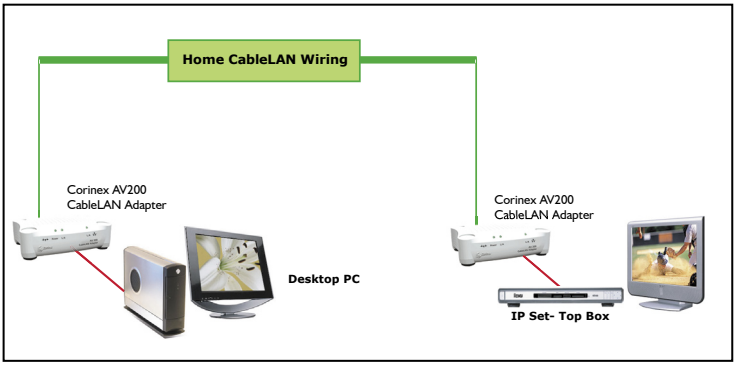
- Configure the Access Point:
  - Set its **IP** address.
  - Select In-Home AV **MAC**.
  - Select **AP** from the Access NVRAM Node list.
  - Select the spectral configuration (notches either enabled or disabled).
  - Add the authorized End Points to the Allowed MAC Address list.
  - Select a unique **Network Number**, which will be used by all devices connecting to this Access Point.

- Configure the required End Points:
  - Set their **IP** addresses.
  - Select In-Home AV **MAC**.
  - Select **EP** from the Access NVRAM Node list.
  - Select the same spectral configuration as you did for the Access Point. (notches either enabled or disabled)
  - Select the same **Network Number** as you did for the Access Point.

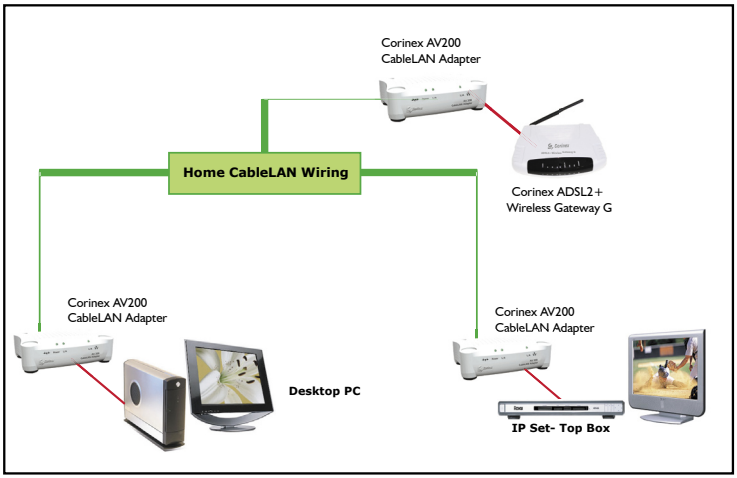
4.3 Home Scenarios

Two possible home scenarios were chosen as examples to demonstrate the capabilities of *In-Home AV networks*. The two setups are presented and explained below.

The picture below exhibits a simple CableLAN network where two adapters are used to make the Internet connection available in all outlets of the house. This is the simplest case, where no QoS (Quality of Service) configuration is required.



The next picture shows a more advanced CableLAN network with three *Corinex AV200 CableLAN Adapters*. This is a common network configuration, where Internet access and digital video are delivered through the same ADSL line. This configuration requires some QoS (Quality of Service) settings to guarantee video quality when the network is carrying large amounts of data from the Internet connection.



Any of these two basic scenarios can be enlarged, adding more adapters, computers and set-top boxes.

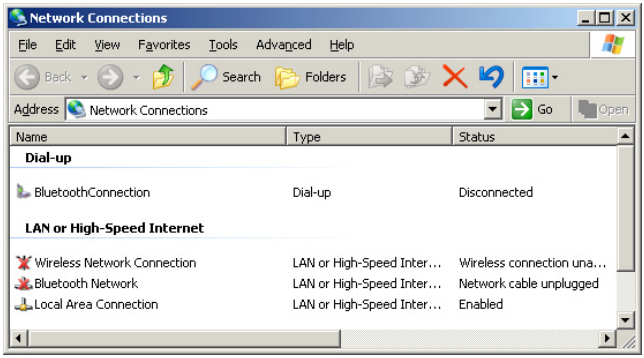
5 Network Configuration

5.1 Setting an IP Address in your computer

This section explains how to set a static IP in your computer's operating system, in order to connect to the AV200 CableLAN Adapter and configure it.

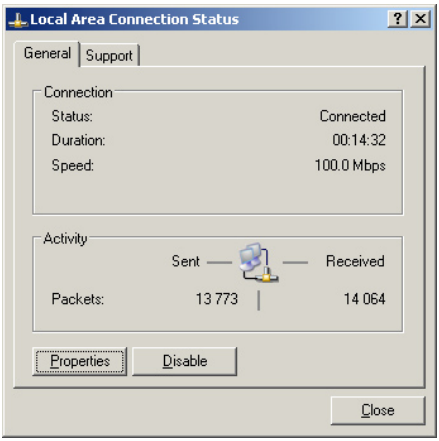
5.1.1 Setting up a static IP in Windows XP

1. Click the **Start** button, open the **Control Panel**. From there, click the **Network Connections** icon and then the **Network Connections** window appears.

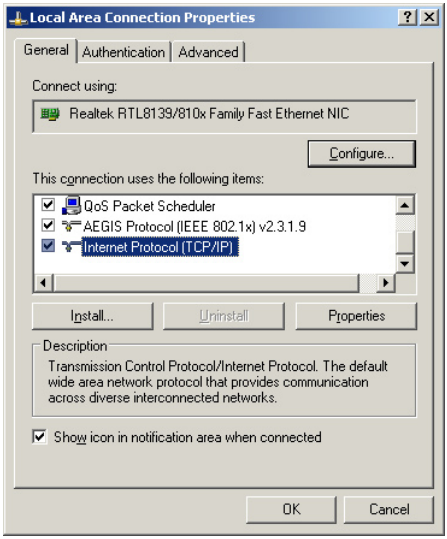


2. Select the **Local Area Connection** icon for the applicable adapter. Double-click the **Local Area Connection**.

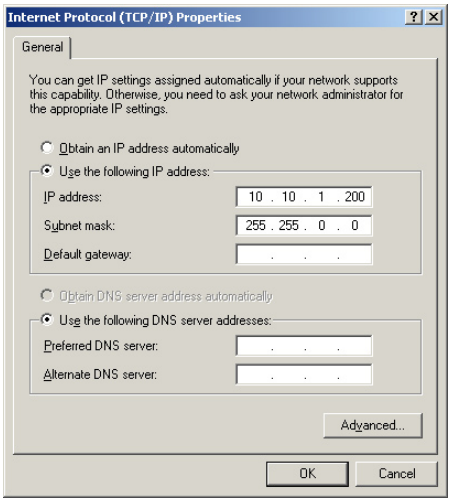
3. The **Local Area Connection Status** screen will appear. Click the **Properties** button.



4. Select **Internet Protocol (TCP/IP)** and click the **Properties** button.



5. Select **Use the following IP address**. Set the **IP address** manually in the format 10.10.1.X (for example 10.10.1.200) and mask 255.255.0.0 of local TCP/IP settings. The **Default gateway** box can be empty.

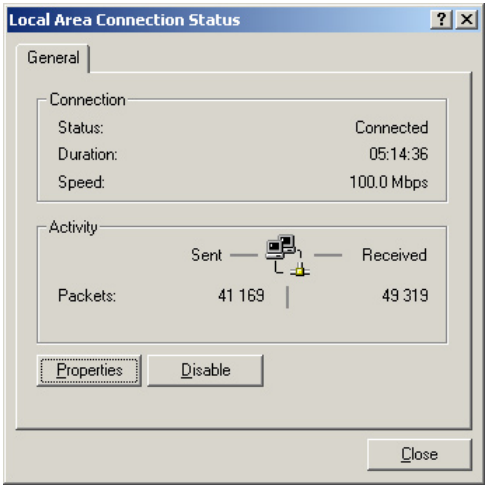


6. Click **OK** button in the TCP/IP Properties window to complete the PC configuration, and click **Close** or the **OK** button to close the Network window.

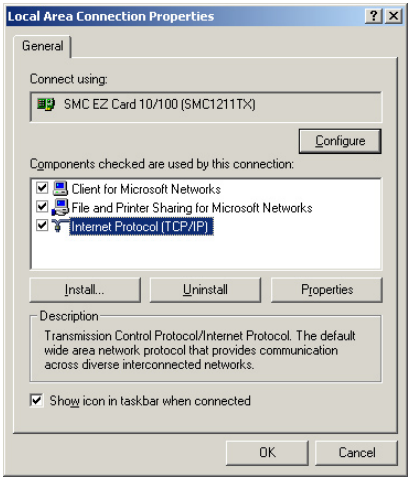
5.1.2 Setting up a static IP in Windows 2000

1. Go to the **network** screen by clicking the **Start** button. Click **Settings** and then **Control Panel**. From there, double-click the **Network** and **Dial-up Connections** icon.

2. Select the **Network and Dial-up Connections** icon for the applicable CableLAN adapter (usually it is the first Local Area Connection listed). Do not choose a TCP/IP entry which name mentions DUN, PPPoE, VPN, or AOL. Double click the **Local Area Connection**. The following window will appear.

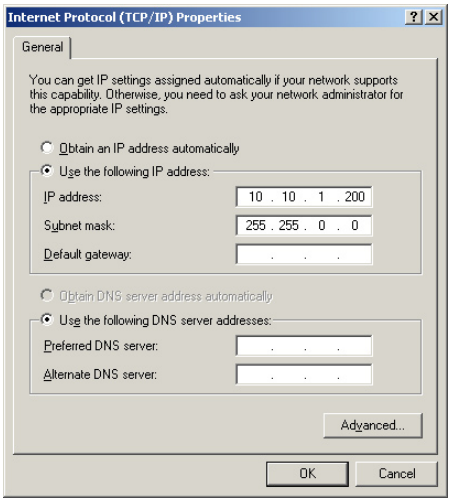


3. Click the **Properties** button to get to the Local Area Connection Properties.



4. Select **Internet Protocol (TCP/IP)** and click the **Properties** button.

5. Select **Use the following IP address**. Set the **IP address** manually in the format 10.10.1.X (for example 10.10.1.200) and mask 255.255.0.0 of local TCP/IP settings. The **Default gateway** box can be left empty.



6. Click the **OK** button in the TCP/IP Properties window to complete the PC configuration, and click **Close** or the **OK** button to close the Network window.

5.1.3 Setting up a static IP in Windows 98

1. Go to the **network** screen by clicking the **Start** button. Click **Settings** and then **Control Panel**. From there, double-click the **Network** icon.

2. On the **Configuration tab**, select the **TCP/IP** line for the applicable CableLAN adapter. Do not choose a TCP/IP entry that mention DUN, PPPoE, VPN, or AOL names. If the word TCP/IP appears by itself, select this line. If there is no TCP/IP line listed, please refer to your Adapter's User Guide on how to install TCP/IP protocol. Click the **Properties** button.

3. If you do not have DHCP server on the network, then select **Use the following IP address**. Set the **IP address** manually in the format 10.10.1.X (e.g. 10.10.1.200) and mask 255.255.0.0 of local TCP/IP settings and click the **OK button**.

4. Click the **OK** button again. Windows may ask you for the original Windows installation disk or additional files. Supply them by pointing to the correct file location, e.g., D:\win98, D:\win9x, c:\windows\options\cabs, etc. (if "D" is the letter of your CD-ROM drive).

5. Windows may ask you to restart your PC. Click the **Yes** button. If Windows does not ask you to restart, restart your computer anyway.

5.1.4 Setting up a static IP in Linux

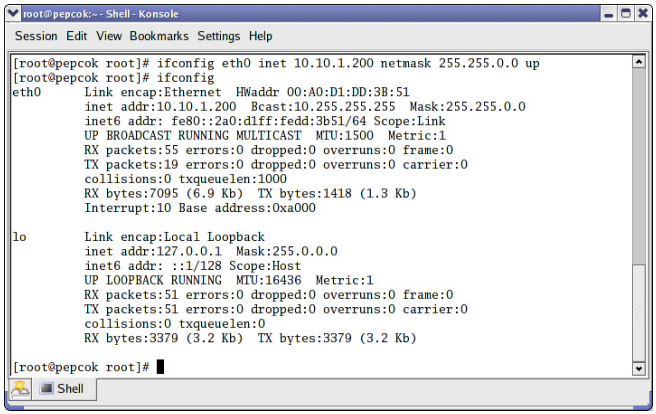
1. You have to be logged in as root in order to change the IP address in your Linux system.

2. Enter the console if you are using some graphical user interface (KDE, Gnome).

3. To change the IP address to 10.10.1.200, enter the command:

   ifconfig eth0 inet 10.10.1.200 netmask 255.255.0.0 up

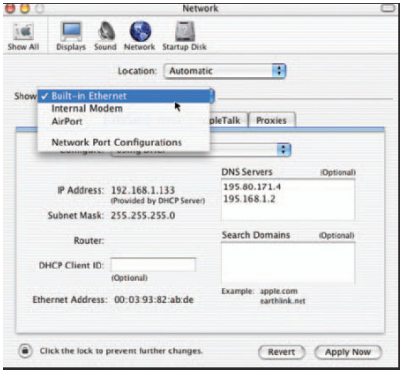
   and press **Enter**. The previous command takes eth0 as the name of the Ethernet interface and may be different on your system. You can check the status of all network interfaces by executing the command **ifconfig** on the console.



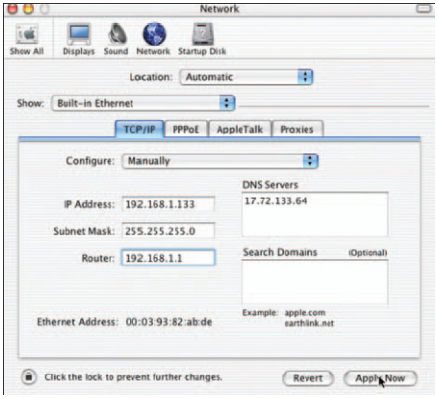
5.1.5 Setting up a static IP in Mac OS X

1. Open the **Network** Control Panel in **System Preferences**.

2. Select **Built-in Ethernet** from the pop-up menu.



3. Set the **IP address** manually in the format 10.10.1.X (e.g. 10.10.1.200) and **Subnet Mask** 255.255.0.0



4. Click on **Apply Now** and close the **Network** panel, saving your settings.

5.2 Improving FTP performance

The latency of a CableLAN network is higher than that of an Ethernet network. Most operating systems have a default setting of the network latency based on Ethernet figures. To obtain the maximum performance using TCP traffic (FTP download, for example) the operating system has to be tuned to the new network conditions.

With a Windows PC, simply double-click on the file **tcpwin.reg**, provided with the modem. With a Linux PC, execute **tcpwin.sh** logged in as root. In both cases the PC has to be reset.

If you do not have these files, they can be created by copying the contents presented below:

TCPWIN.REG

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]
"TcpWindowSize"=dword:00080000
"GlobalMaxTcpWindowSize"=dword:00080000
"Tcp1323Opts"=dword:00000003
```

TCPWIN.SH

```
$wind = (int)($ARGV[0] * 1024);

`echo $wind > /proc/sys/net/core/rmem_default`;
`echo 8388608 > /proc/sys/net/core/rmem_max`;
`echo $wind > /proc/sys/net/core/wmem_default`;
`echo 8388608 > /proc/sys/net/core/wmem_max`;

`echo 4096 $wind 8388608 > /proc/sys/net/ipv4/tcp_rmem`;
`echo 4096 $wind 8388608 > /proc/sys/net/ipv4/tcp_wmem`;
`echo 8388608 8388608 8388608 > /proc/sys/net/ipv4/tcp_mem`;
```

To use this script in Linux, you must have kernel 2.4. Logged in as root, execute the following command:

./tcpwin.sh 512

This will set the TCP window to a size of 512 Kilobytes.

5.3 Checking Network Performance

On the **Main** page, under the heading **Available CableLAN Connections**, there is a list of the MAC addresses of all of the neighboring adapters that have a connection with that adapter. The list also indicates the physical throughput (actual data rate), in terms of both transmission and reception, that the adapter is achieving with each adapter on the network.

Available Cablelan Connections

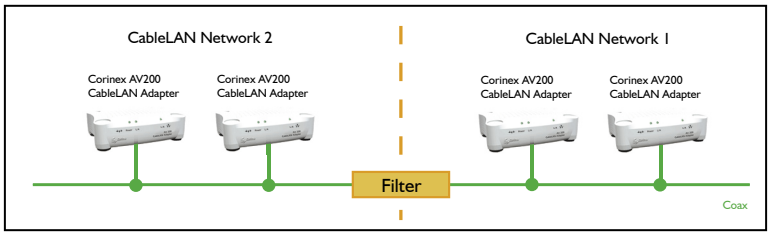
Port	MAC Address	Phy Tx Throughput	Phy Rx Throughput	Bridge State
10	0050C22CF6B8	116 Mbps	114 Mbps	Forwarding
9	0050C22CF6C6	112 Mbps	110 Mbps	Forwarding

5.4 Using Coaxial Filters

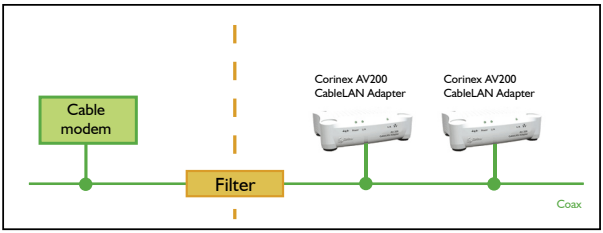
A coax filter is a high-pass filter which allows only the TV signal through. This filter blocks the AV CableLAN signal (2-34 MHz).

When to use this filter:

- When you want to isolate your AV CableLAN network from the rest of the coaxial infrastructure, either because you don't want the CableLAN signal from your network to go out and disrupt other adapters, or because you want to isolate this network from the noise, or other traffic, in the rest of the cable network.



- When you want to isolate the AV CableLAN network from interference caused by a Docsis modem, you put the filter between the Docsis modem and the AV CableLAN network.



6 Troubleshooting Guide

The *Corinex AV200 CableLAN Adapter* has been designed to be a reliable and easy-to-use network connection device. Please refer to the list below to aid in troubleshooting.

The POWER LED is off.

1. Verify the connection of the power cable to the adapter's power inlet.
2. Make sure the power adapter is properly plugged directly into the electrical outlet, and that the outlet has power.
3. Try another outlet.

The CableLAN Act LED is off.

1. Make sure there is no analogue TV amplifier or too many T-splitters between the AV200 CableLAN adapters which should communicate.
2. Try to connect two AV200 CableLAN adapters with a short coaxial cable for a short test to check the connectivity.

The Ethernet LED is off.

1. Make sure the adapter is connected with an Ethernet enabled device with an RJ-45 cable and both devices are powered.

If the trouble persists, please visit **www.corinex.com** and go to the appropriate section for information on your product. There you will find news, manuals and software updates, as well as frequently asked questions (FAQ).

To avoid personal injury and damage to the system:

1. The principal method to disconnect the device completely from the electrical power network (mains) is to unplug the power cord from the mains socket.
2. Never install the unit in wet areas or next to radiators/heaters.
3. Never use the unit outside.
4. Unplug the unit during severe storms.
5. Never open the equipment enclosure.

If you can't solve your difficulties using the information sources mentioned above, please send us the problem description via **http://www.corinex.com/web/com.nsf/Doc**. We would like you to give us all possible information about your devices and your network, when contacting us. This includes:

- Types of devices you have, if possible with serial numbers (printed on the safety labels)
- Which of these devices are working incorrectly or don't work at all (indicate the problem)
- If it's possible, send us a scheme of your network topology also with the IP addresses for computers/router/access point, as this can speed up the problem diagnosis. If you use any non-Corinex equipment, please specify what kind. Illustrations can be made in any graphics editor, exported to one of the standard graphic formats (JPEG, GIF). Or you can just draw it on paper and scan it
- Specify operating systems used with the devices
- Please send us the firmware version and configuration of these devices. Please see the user guide for detailed instructions on this.